Password Security is the Key to System and Force Protection

October 2005

Passwords are much like the keys to your house or car. They enable you to keep important things secure and protected from would be intruders. For that reason you want them to have the same attributes. They must be unique, so that they don't provide access to multiple places. They need to be kept physically secure, so that they do not fall into the wrong hands. They must be made complex, so that they are not easily reproduced. Passwords to Army systems require the same high level of attention and security as the keys that protect your family, your property and yourself.

As the accompanying cartoon demonstrates, the physical security of your passwords is critical to their effectiveness. Under no circumstances should passwords be stored where they can be accessed and compromised. Unfortunately the carton depicts a dangerous common occurrence. If soldiers can remember baseball statistics, the birthdays of all their cousins, and the detailed engine attributes of every model of Mustang sports car, they can remember 10-character, case sensitive passwords, as required by AR 25-2. These passwords guard the safety and security of their fellow soldiers and their country. They need to be created and protected accordingly.

Effective passwords have important security features that must be implemented and maintained. They need to be a combination of uppercase letters, lowercase letters, numbers, and special characters, including at least two of each of the four types of characters, for example, x$TloTBn2!. Passwords must not include such references as social security numbers (SSNs), birthdays, USERIDs, names, slang, military acronyms, call signs, dictionary words, consecutive or repetitive characters, system identification, or names. They also need to be complex to prevent them from being easy to guess, for example, mypassword or abcde12345.

All default, system, factory installed, function-key embedded, or maintenance passwords must be changed to a secure password immediately. Also, password expiration must be not more than 150 days.

As easy as it might seem, password security is often overlooked or discounted. The CERT/CC (Computer Emergency Response Team / Coordination Center), a federally funded organization based at Carnegie Mellon University, estimates that 80% of all network security problems are caused by bad passwords. A typical weak password is short and consists solely of letters in a single case. What may seem fine for an AOL account, it is absolutely unacceptable for protecting national interests. Good passwords are the simplest and most important part of information security.

Understandably, a soldier's life is filled with passwords, both personal and military. Regardless of a person's ability to keep them all memorized – in addition to the baseball statistics and birthdays – it can become difficult to keep them all straight. This could lead to confusion at a critical moment. In response to this situation, the Homeland Security Presidential Directive (HSPD-12) of August 2004 directs the Secretary of Commerce to establish a policy for a common, secure identification standard for all federal agencies including the military. This directive should establish a uniform procedure that will make password security more manageable while retaining it effectiveness.

Passwords keep the door to our critical systems securely closed. Like locks, they don't provide total protection. However, they are effective deterrents to intruders. Combined with the other security procedures laid out in AR 25-2, they create an effective defense against hackers and our enemies. Secure and effective passwords, like house keys, deserve and require the attention and protection of every soldier.